FortiADC™ v4.0 Patch Release 5

E Series

Release Notes

FortiADC 4.0 Patch Release 5 E Series Release Notes

October 20, 2014

Revision 1

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log **4**

Introduction **5**

Supported Hardware 5

Resolved Issues **6**

Known Issues **8**

Product Registration **11**

Image Checksums **13**

Change Log

Date	Change Description
October 20, 2014	Initial Release (FortiADC-E 4.0 Patch Release 5)

Introduction

This document lists the resolved and known issues for FortiADC E Series v4.0 build 0027. FortiADC provides load balancing, both locally and globally, and application delivery control.

For additional documentation, please visit:

http://help.fortinet.com/fadc.html

Supported Hardware

This release of the FortiADC E Series software is an update release for all FortiADC-E Series hardware (300E, 400E, 600E, 1000E).

Resolved Issues

This release addresses a major security vulnerability. See Bug ID 9011 on the following page. All customers should upgrade to this release as soon as possible.

This section lists the major issues that have been fixed since the last release. For inquires about a particular bug, please contact Customer Support.

Table 1: Resolved Issues.

Bug ID	Description
8609 8886	**Troubleshooting**: Added additional SSL / HTTPS debugging information to save state archives to aid in problem analysis.
8857	**Failover**: In certain cases where both systems are attempting to assume primary mode, traffic is sent to the backup system instead of the system that actually became primary. Failover has been modified so that whenever a system assumes primary mode, it will always send out Gratuitous ARPs for all the IP addresses it owns. (1097050)
8859	**Restore**: Restoring a backup archive taken on one model to another model results in limited or no network availability after the restore is complete. This bug has been fixed
8875	**Restore and Failover**: Failover does not always re-configure itself properly in this scenario: 1. Assume two units (A, B) are in failover. 2. Unit A is taken offline. 3. A new unit (C) is brought online to replace unit A, and a backup archive from unit A is restored onto unit C. 4. Unit C is then powered off, and unit A is brought back online. After the last step above, failover between the units A and B is not established properly. This bug has been fixed. (1082880) [Note that if unit A was only disconnected from the network and not shut down during Step 2 above, a reboot of unit A in Step 4 will be required in order to synchronize failover between the two units properly.]
8882	**Active-Active Failover**: Fixed issues that could prevent one or more units from entering failover when several peers are added quickly to the configuration.
8890	**Troubleshooting**: Taking a save state archive on some systems can impact the system's ability to process incoming connections during periods of high traffic. This bug has been fixed. (1156042)
8896	**Failover**: Fixed an issue that could cause all peers to go into backup mode if the failover IP address was also being used in a subnet NAT (Network Address Translation) rule. (1097050)

8903	**Networking**: Errors like the following may be seen in the system log: wm7: MDIC write error: phy 1 reg 9 wm7: MDIC write error: phy 1 reg 4 This was isolated to an error in the wm() interface driver and has been fixed. (1097050)
9011	**Security Vulnerability**: A platform-specific security vulnerability has been discovered that permits a remote attacker to gain access to currently configured subnets. An unprivileged user may be able to inject packets into any network configured on FortiADC, or may be able to communicate with hosts present on networks configured on FortiADC. This vulnerability is present on all FortiADC-E models running any release since (and including) 3.1.1. (1230888)

Known Issues

This section lists the major known issues in this release, but is not a complete list. For inquires about a particular bug, please contact Customer Support.

Table 2: Known Issues.

Bug ID	Description
3351 3989	**Match Rules**: debug_message(), ssl2(), ssl3(), and tls1() functions (supported in Version 8) are not accepted for expressions.
3468	**Clusters**: The 'Reset on server failure' global option supported in previous releases is not yet implemented in Version 10.
4101	**Layer 4 UDP clusters**: The 'persist override' flag on UDP cluster server instances does not override persistence.
5393	**TCP/ACV Health Checks**: The CLI and Web UI will indicate that a server instance is 'ACV DOWN' (or not responding to ACV probes) even when ACV is not set, when the server is not responding to TCP probes. It should be shown as 'L4 TCP DOWN'. In any case, the server is correctly marked 'down'.
5663	**Health Checks**: In a server pool configuration, do not define more than 16 health check instances per server instance. If 17 health check instances are defined on a server instance, the system will become unresponsive and reboot. The workaround, after the system comes back up, is to remove the 17th health check from the configuration file. This bug will be fixed in a future release.
6385	**VMware Integration**: In a VMware configuration where Microsoft Active Directory is used, logging in to VMware will fail if the VMware account used to log into VMware is defined within an Active Directory domain. On VMware the login succeeds, but from FortiADC the login attempt fails. If you test the login, it will appear to hang. Messages like the following appear in the log: "vlbd[22043]: |e|v vCenter;|75000039: unable to send message|Message too long|".The workaround is to use a VMware account that is not defined within Active Directory to log into VMware.
6583	**Modifying VLAN MTU**: If you modify a **VLAN MTU** parameter to a value that is lower than the currently set value, you must reboot to ensure proper operation of the network interface.
6467	**Layer 4 UDP clusters**: A server defined on the ADC cannot access any UDP clusters defined on the ADC. This bug will be fixed in a future release.
6648	**Responders**: It is not possible to enter a regular expression containing a "?" character using the CLI. The workaround is to use the Web UI instead
6669	**SSH**: When using SSH to log into the CLI, the file editor (for certificates, responders, etc.) may not work. This may be due to the terminal type presented to the system on login. To work around this issue, modify your terminal emulator settings before logging in and set the terminal type to 'xterm'.
6966	**Web UI**: Cannot define an SNMP Trap server in the Web UI. The workaround is to use the CLI.

7363	**Web UI**: Some CLI commands are not supported by the CLI Console widget in the Web UI Dashboard. See the online WebHelp for more information.
7599	**Subnet destination (or policy) routes** have been removed (see bug 7556, above). That feature included the ability to specify the source IP address to use for a packet routed to another network. Now, the system automatically configures destination routes, and uses the subnet IP address as the source IP address. The capability to specify a source IP address will be provided in a future release.
7656	**Web UI**: When using Internet Explorer 11 to view the Web UI, issues have been observed where UI source code is displayed and a page is unusable. The only workarounds are to either try Compatibility Mode, use Internet Explorer 10, or use another browser.
7750	**FTP Clusters**: The IP address and port for an FTP cluster (a TCP cluster with a start port of 21) cannot be modified. The workaround is to create a new FTP cluster.
7814	**Failover**: The per-subnet 'command' flag has been moved in the CLI to a new 'failover' context. This flag must currently be managed through the CLI. In the Web UI, this flag remains on the subnet configuration tab. Attempting to disable the flag in the Web UI appears to succeed, but if the tab is redisplayed the flag is still set on that subnet. This issue in the Web UI will be fixed in a subsequent release.
7830	**VLAN MTU**: The VLAN MTU parameter currently cannot be set above 4839.
7896	**Smart Controls**: For scheduled Smart Controls, modifying an existing schedule specification does not work correctly; the configuration file is updated properly, but the existing schedule is not removed from the running system. The Smart Control ends up with two schedules, only one of which is apparent to the user. There are two workarounds: • Remove the Smart Control and re-create it with the correct schedule. • Reboot the system after modifying the Smart Control's schedule. This bug will be fixed in a future release.
7923	**Preferred static routes**: If the user adds a '0/0' static route and a preferred static route for a server with the same gateway, then the preferred static route is ignored.
8657	**SSL Ciphers**: The cipher has been temporarily disabled for all HTTPS clusters due to reconnection issues: • AES256-GCM-SHA384
8579	**Backup of Large Configurations (Web UI only)**: Creating a 'local' backup archive (intended to be saved through the user's browser on the local system) fails for large configurations containing hundreds of objects. The workaround is to create the archive using the FTP or HTTP transfer alternatives.
8676	**Upgrade using Local File in Web UI**: When upgrading using a 'Local File' uploaded to the system via the browser, the system displays a popup that says: 'Downloading the upgrade archive…'. If the system runs out of space in the filestore, this popup will appear and never be dismissed. Also, a message in the system log will appear: `command phpcgi, on /var/crash: file system full` If this occurs, you must remove files from the filestore (using the CLI) so that there is at least 50MB of space in the filestore. Then, re-try the upgrade and it should now succeed.

8744	**Alerts for LLB Gateways**: It is possible to create an alert for a state transition (up/down) on an LLB Gateway, but the alert will never fire because of internal issues. This will be fixed in a future release. (1097050)
8822	**IP Reputation:** The 'show' command does not work in the 'rep-blk' context. The workaround is to issue the show command from the global context: `eqcli> **show reputation block**`

Product Registration

Product registration has been changed from previous releases to use the FortiCare system. Fortinet customer services (such as firmware updates and technical support) require product registration. Take a moment now to register your product at the Fortinet Customer Service and Support web site:

https://support.fortinet.com

Before you can register, you will need:

1. **Access to a new or existing Support Account**. Information on how to create and manage a support account is provided in the Fortinet Support Portal User Guide. If your organization already has an account, obtain the user name and password information from your local account administrator to log in.
2. **The serial number of the unit you want to register**. You can find this information using either the CLI or the GUI after powering up your appliance:
   - To use the CLI, log in to the CLI (over the serial console or, if networking is configured, using SSH over an appropriately configured subnet) and enter the following CLI command:

     ```
     eqcli > version
     ```

     Record the **System Serial Number** from the command output.
   - If networking is configured and the GUI has been enabled on a subnet., you can also get the serial number from the 'System Information' widget on the GUI dashboard. The Dashboard appears automatically when you log into the GUI.

Once you have obtained both the login credentials of a support account and the System Serial Number of the unit to register, do the following:

1. Log in to https://support.fortinet.com using the login credentials obtained above.
2. Follow the instructions provided in the Registration Frequently Asked Questions under the heading "How do I register a Fortinet device?". When requested, enter the **System Serial Number** you obtained above into the appropriate form. Once registration is completed, the appliance serial number and other information will appear in the **FortiCare Registration** area.

Your system is now registered. If your system can connect to the internet, you can now update the support information displayed in the CLI and GUI by doing one of the following:

- In the CLI, enter the following to update the support information on your unit:

  ```
  eqcli > forticare registration
  ```

  View the updated **Support information** (including **Last refresh date**, **Support end**, and **Email)** by entering:

  ```
  eqcli > version
  ```

- In the GUI, select the **System** configuration tab on the left navigational pane and then click on **Global > Dashboard**. The System information widget on the right pane will indicate the **Support information** (including **Last refresh date**, **Support end**, and **Email)**. Click on the **Refresh** button to update the registration information.

Note that the registration information does not update automatically in either the CLI or the GUI; you must use either the CLI '`forticare registration`' command or the **Refresh** button in the GUI Dashboard's **System Information** widget to update.

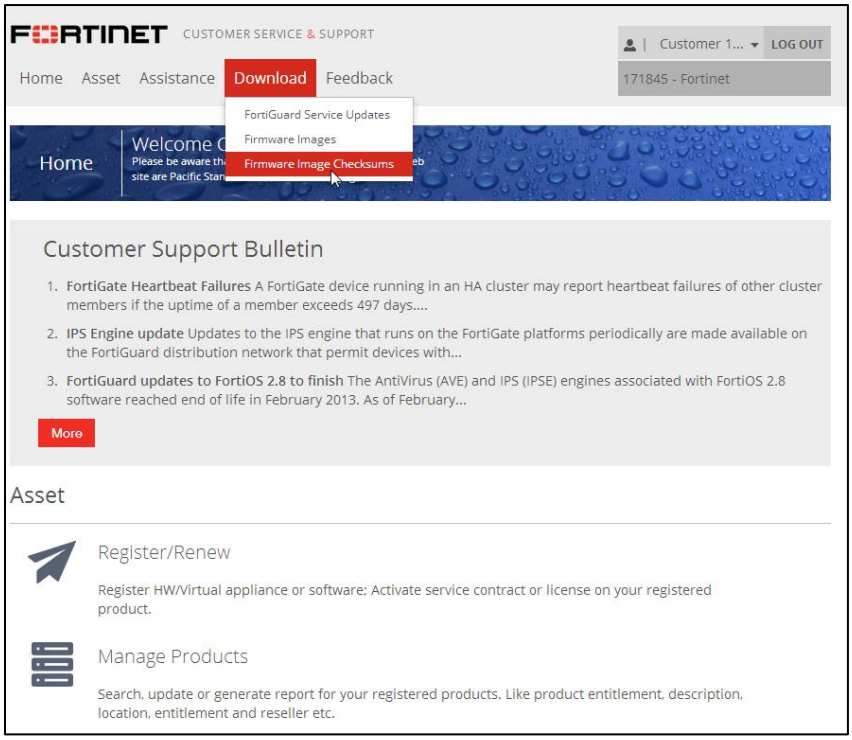
Image Checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

Figure 1: Customer Service & Support image checksum tool


FORTINET
CUSTOMER SERVICE & SUPPORT
Customer 1...
LOG OUT
Home
Asset
Assistance
Download
Feedback
171845 - Fortinet
FortiGuard Service Updates
Firmware Images
Firmware Image Checksums
Home
Customer Support Bulletin
1. FortiGate Heartbeat Failures A FortiGate device running in an HA cluster may report heartbeat failures of other cluster members if the uptime of a member exceeds 497 days....
2. IPS Engine update Updates to the IPS engine that runs on the FortiGate platforms periodically are made available on the FortiGuard distribution network that permit devices with...
3. FortiGuard updates to FortiOS 2.8 to finish The AntiVirus (AVE) and IPS (IPSE) engines associated with FortiOS 2.8 software reached end of life in February 2013. As of February...
More
Asset
Register/Renew
Register HW/Virtual appliance or software; Activate service contract or license on your registered product.
Manage Products
Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

After logging in to the web site, in the menus at the top of the page, click *Download*, then click *Firmware Image Checksums*.

Alternatively, near the bottom of the page, click the *Firmware Image Checksums* button. (The button appears only if one or more of your devices has a current support contract.) In the *File Name* field, enter the firmware image file name (including its extension), then click *Get Checksum Code*.